

AMENDMENTS TO THE CLAIMS

The below listing of claims will replace all prior versions, and listings, of claims in the subject application:

Listing of Claims:

1. (Original) A method comprising:

receiving content comprising a set of attributes having L through N levels of access, where $L < N$, and content at a given level of access being decryptable by a corresponding key;

receiving a base key corresponding to an M of N level of access, where $L \leq M \leq N$; and

deriving lower level keys based on the base key, the lower level keys being used to access content having an M level of access or lower.
2. (Original) The method of claim 1, additionally comprising receiving a D-dimensional matrix for each attribute in the set of attributes, wherein D corresponds to a number of attributes of the content, and wherein the matrix comprises matrix values for determining how to generate a key corresponding to a given section of the content, and said deriving lower level keys based on the base key comprises, for a given lower level key, using a function based on a matrix value corresponding to the lower level key and a one-way hash function of an adjacent higher level key.

3. (Original) The method of claim 1, wherein said deriving lower level keys based on the base key comprises, for a given lower level key, using a modular exponentiation of a higher level key.

4.-10. (Cancelled)

11. (Original) A machine-readable medium having stored thereon data
* representing sequences of instructions, the sequences of instructions which, when executed by a processor, cause the processor to perform the following:

receive content comprising a set of attributes having L through N levels of access, where $L < N$, and content at a given level of access being decryptable by a corresponding key;

receive a base key corresponding to an M of N level of access, where $L \leq M \leq N$; and

„ derive lower level keys based on the base key, the lower level keys being used to access content having an M level of access of lower.

12. (Currently Amended) The machine-readable medium method of claim 11, additionally comprising instructions that cause the processor to receive a D-dimensional matrix for each attribute in the set of attributes, wherein D corresponds to a number of attributes of the content, and wherein the matrix comprises matrix values for determining how to generate a key corresponding to a given section of the content, and the instructions cause

- the processor to derive lower level keys based on the base key comprises,
for a given lower level key, using a function based on a matrix value
corresponding to the lower level key and a one-way function of an
adjacent higher level key.
13. (Currently Amended) The machine-readable medium method of claim 11,
wherein the instructions cause the processor to derive lower level keys
based on the base key comprises, for a given lower level key, by using a
modular exponentiation of a higher level key.
14. (Original) An apparatus comprising:
- at least one processor; and
 - a machine-readable medium having instructions encoded thereon, which
when executed by the processor, are capable of directing the
processor to:
 - receive content comprising a set of attributes having L through N
levels of access, where $L < N$, and content at a given level of
access being decryptable by a corresponding key;
 - receive a base key corresponding to an M of N level of access,
where $L \leq M \leq N$; and
 - derive lower level keys based on the base key, the lower level keys
being used to access content having an M level of access of

lower.

15. (Currently Amended) The apparatus method of claim 14, additionally comprising instructions that cause the processor to receive a D-dimensional matrix for each attribute in the set of attributes, wherein D corresponds to a number of attributes of the content, and wherein the matrix comprises matrix values for determining how to generate a key corresponding to a given section of the content, and the instructions cause the processor to derive lower level keys based on the base key comprises, for a given lower level key, using a function based on a matrix value corresponding to the lower level key and a one-way hash function of an adjacent higher level key.
16. (Currently Amended) The apparatus method of claim 14, wherein the instructions cause the processor to derive lower level keys based on the base key comprises, for a given lower level key, by using a modular exponentiation of a higher level key.
- 17.-19. (Cancelled)
20. (Original) A method comprising:
- receiving encrypted content comprising a set of attributes having L through N levels of access, where $L < N$, and each level being accessible by a corresponding key;
- receiving a base key corresponding to an M of N level of access, where

$L \leq M \leq N$;

deriving lower level keys based on the base key, the lower level keys
being used to access content having an M level of access or lower;
and

using a given lower level key to decrypt the content at a corresponding
level.

21. (Original) The method of claim 20, additionally comprising receiving a D-dimensional matrix for each attribute in the set of attributes, wherein D corresponds to a number of attributes of the content, and wherein the matrix comprises matrix values for determining how to generate a key corresponding to a given section of the content, and said deriving lower level keys based on the base key comprises, for a given lower level key, using a function based on a matrix value corresponding to the lower level key and a one-way function of an adjacent higher level key.
22. (Original) The method of claim 20, wherein said deriving lower level keys based on the base key comprises, for a given lower level key, using a modular exponentiation of a higher level key.